Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

First draft (30 May 2007)

Cybercrime legislation – country profile

Brazil

This profile has been prepared within the framework of the Council of Europe's Project on Cybercrime in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the country covered or of the Council of Europe.

Comments may be sent to:

Alexander Seger
Department of Technical Cooperation
Directorate General of Human Rights and Legal Affairs
Council of Europe, Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

Country:	**Brazil**
Signature of Convention:	No
Ratification/accession:	No What measure are being undertaken in your country to become a Party? The Ministry of External Relations, The Ministry of Justice (by Federal Police Department (DPF) and International Cooperation and Assets Recovery Department (DRCI)), the Office of Institutional Security of The Presidency of Republic (GSI), The Science and Technology Ministry (MCT) and The Parliament, where is running a legislative project, are involved in analysis of the Convention on Cybercrime. What specific obstacles (legislative or other) prevent ratification/accession? Natural delay of legislative process and multiple laws about specific crimes.
Provisions of the Convention	***Corrresponding provisions/solutions in national legislation*** *(pls quote or summarise briefly; pls attach relevant extracts as an appendix)*
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data"	Definitions to be included / adopted after approval by Congress "Computer system", "computer data", "traffic data" – terms defined in art. 154 C of the Brazilian Criminal Law, as amended by art. 3 of the Substitute Amendment to Senate bills PLS 76/2000 and PLS 137/2000, in addition to House bill PLC 89/2003, from now on referred to as Substitute, that will be effective after it is passed by Congress; "service provider", is defined in art. 3, Law n. 8078/1990 – Consumer

	Protection Code
Chapter II – Measures to be taken at the national level *Section 1 – Substantive criminal law*	
Article 2 – Illegal access	Measures adopted to establish illegal access as a criminal offence,. Provided for in art. 154-A of the Brazilian Criminal Law, as amended by art. 3 of the Substitute Amendment. Art. 154-A is generic and includes provisions as per art. 2 of the Convention; art. 154-B corresponds to illegal access in its aggravated form as provided for in the second part of art. 2 of the Convention. Art. 155, paragraph (4), item V, of the Brazilian Criminal Law, as amended by art. 4 of the Substitute Amendment, provides for digital larceny (illegal access to data) through unauthorized use of password , which according to the Convention, is to be treated as computer damage or data interference.
Article 3 – Illegal interception	Measures adopted to establish illegal interception as a criminal offence. Law n. 9296 (24th. July, 1996), currently in force, in its art. 10, already establishes the interception of telephone, computer or telematic transmissions as criminal offences. and now, in compliance with art. 16 of the Substitute Amendment, such offences punished with detention shall be included.
Article 4 – Data interference	To be clarified. No new specific rule has been established; art.163 of the Criminal Code is assumed to be applicable (offence of criminal damage); art. 183-A is to be added to the Code, in compliance with art. 7 of the Substitute Amendment, which additionally provides for other objects of criminal offence (wrongful damage, deletion, deterioration, alteration or suppression): the data, information, stored database, computer network and other relevant computer elements.
Article 5 – System interference	To be clarified. Brazilian criminal law is well-founded on the matter of legal principle, requiring a clear definition of forbidden conduct. Therefore, no generic provision has been devised for system interference, or computer sabotage. It has been decided to extend to computer offences the already existing typification of crimes against security and operation, and crime of interruption or disruption (...), impediment or hindrance to reestablishment ... provided for in articles 265 and 266 of the Criminal Code, as amended by art. 8 of the Substitute Amendment.
Article 6 – Misuse of devices	To be clarified. No generic provision has been established for misuse of devices as per the wording of the Convention on Cybercrime. It has been decided to typify two concrete offences in art. 2 of the Substitute Amendment, which amends the Criminal Code, art. 163-A (create, insert or expose malicious code...) and art. 171-A (disclose malicious code with the intention of fraud), reveal by any means whatever, a program, set of instructions or computerized system with the purpose to induce in error in any way or, …….. to obtain an illegal advantage, therefore causing harm to a third party:). For the part the Substitute has not provided for, the Convention, in its art. 6, (3), provides for the possibility of reserving the right not to apply paragraph 1 of art. 6.
Article 7 – Computer-related forgery	Measures adopted to establish computer-related forgery as a criminal offence by the general provisions of the Criminal Code. No specific provisions in the Substitute Amendment were devised to address art. 7 of the Convention. It has been decided to include the

	penalty for the offences mentioned herein in the general provisions on offences of fraud (larceny by fraud, art.171 of the current Criminal Code) and forgery (counterfeit another person's private documents, art. 298 of the current Criminal Code). In its art. 9 and 10, the Substitute Amendment has provided for special forgery offences, to amend art. 298, sole paragraph, and art. 298-A of the Criminal Code.
Article 8 – Computer-related fraud	Measures adopted to establish computer-related forgery as a criminal offence by the general provisions of the Criminal Code. No specific provisions in the Substitute Amendment were devised to address this item of the Convention. It has been decided to include the penalty for the offences mentioned herein in the general provisions on offences of fraud (larceny by fraud, art.171 of the current Criminal Code) and forgery (counterfeit another person's private documents, art. 298 of the current Criminal Code). In its art. 9 and 10, the Substitute Amendment has provided for special forgery offences to amend art. 298, sole paragraph, and art. 298-A of the Criminal Code.
Article 9 – Offences related to child pornography	Measures adopted in part. Art. 241 of Law n. 8069, of July 13th.,1990, as amended by Law n. 10764, of November 12th, 2003, punishes most of the offences typified as per art. 9 of the Convention (art. 241. - Cause the appearance, produce, sell, supply, expose or transmit by any means of communication whatever, including the world wide web or internet, pornographic photographs or images or scenes of explicit sexual activity involving children or adolescents. Provisions as per paragraph 1, d) and e) and as per paragraph 2, b) and c) of art. 9 of the Convention are hereby excluded. Further on, paragraph 4 provides for the right not to apply above paragraphs and sub-paragraphs.
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights	Measures adopted. Brazilian current legislation already addresses the protection implied in provisions as per art. 10: Law n. 9609 (February 19th.,1998 – Protection of Computer programs), Law n. 9610 (February 19th, 1998 – Protection of Copyrights), and Law n. 10695 (July 1st.,2003 – alters the Criminal Code to include offences related to infringements of copyrights – "Anti-Piracy" Act).
Article 11 – Attempt and aiding or abetting	To be clarified. Provisions implemented in part, in art.154-A, paragraph (1) of the Criminal Code, as amended by art. 3 of the Substitute Amendment,….Paragraph (1). Those who allow, facilitate or supply a third party with non-authorized means of access to a computer network, communications device or computer system shall be liable to the same penalties as the offender.
Article 12 – Corporate liability	Not implemented. The Brazilian criminal law does not address corporate liability unless in the case of offences against the environment.
Article 13 – Sanctions and measures	Measures adopted, except in the case of Art. 12, excluded. The Brazilian Criminal Code and other criminal legislation provide for punishment with imprisonment together with or without fine.
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions	Measures adopted. According to Decree Law n. 3689, October 3rd., 1941 – Code of Penal Procedure (CPP), as amended by art. 17 of the Substitute Amendment

	in reason of amendment of art. 313 of CPP, with the addition of item IV, that extends preventive imprisonment for offences punished by detention, committed against a computer network, communications device or computer system, or committed through the use of a computer network, communications device, or computer system according to criminal law.
Article 15 – Conditions and safeguards	Measures adopted. 1998 Federal Constitution, Art. 5, Fundamental Rights and Guarantees.
Article 16 – Expedited preservation of stored computer data	Measures adopted in part. Art. 21, Item IV of the Substitute Amendment provides for expedited preservation of traffic data, user identification data and communications content.
Article 17 – Expedited preservation and partial disclosure of traffic data	Measures adopted in part. Art. 21, Item IV of the Substitute Amendment provides for expedited preservation of traffic data, user identification data and communications content.
Article 18 – Production order	Measures not adopted. An injunction mechanism has been provided for.
Article 19 – Search and seizure of stored computer data	No specific prevision of adoption. Provisions for Search and Seizure in the digital environment are currently in force as provided for in other legislation.
Article 20 – Real-time collection of traffic data	Measures adopted. Law n. 9296 (24/July/1996), art.1, sole paragraph, provides for the real-time collection of traffic data in computer or telematic systems; and art. 16 of the Substitute Amendment provides for such a collection even in the case of offences punished by detention. Art. 21, Items I, II, III and IV of the Substitute Amendment makes it compulsory for access providers to supply data capable of identifying users and connections when expressly authorized by judicial order during an investigation.
Article 21 – Interception of content data	Measures adopted. Law n. 9296 (24/July/1996), art.1, sole paragraph, provides for the real-time collection of traffic data in computer or telematic systems; and art. 16 of the Substitute Amendment provides for such a collection even in the case of offences punished by detention. Art. 21, Items I, II, III and IV of the Substitute Amendment makes it compulsory for access providers to supply data capable of identifying users and connections when expressly authorized by judicial order during an investigation
Section 3 – Jurisdiction	
Article 22 – Jurisdiction	To be clarified. For purposes of investigation and trial, and according to the body of Supreme Court case law, Brazilian Criminal Law takes into consideration the territory where the consequences of the offence were felt, the territory where the offence was committed being irrelevant.
Chapter III – International co-operation	
Article 24 – Extradition	To be clarified. Art. 780 through 790 of the Brazilian Code of Penal Procedure address jurisdictional issues and relationship with foreign authorities.
Article 25 – General principles relating to mutual assistance	To be clarified. Art. 780 through 790 of the Brazilian Code of Penal Procedure address jurisdictional issues and relationship with foreign authorities.
Article 26 – Spontaneous information	Measures not adopted.
Article 27 – Procedures	To be clarified.

pertaining to mutual assistance requests in the absence of applicable international agreements	Art. 780 through 790 of the Brazilian Code of Penal Procedure address jurisdictional issues and relationship with foreign authorities.
Article 28 – Confidentiality and limitation on use	To be clarified.
Article 29 – Expedited preservation of stored computer data	Measures not adopted. Reference is made to international cooperation, specifically to the expedited preservation of stored computer data in a foreign country, and the expedited preservation and disclosure of stored traffic data.
Article 30 – Expedited disclosure of preserved traffic data	Measures not adopted. Reference is made to international cooperation, specifically to the expedited preservation of stored computer data in a foreign country, and the expedited preservation and disclosure of stored traffic data.
Article 31 – Mutual assistance regarding accessing of stored computer data	Measures not adopted.
Article 32 – Trans-border access to stored computer data with consent or where publicly available	Measures not adopted.
Article 33 – Mutual assistance in the real-time collection of traffic data	Measures not adopted.
Article 34 – Mutual assistance regarding the interception of content data	Measures not adopted.
Article 35 – 24/7 Network	Measures not adopted.
Article 42 – Reservations	